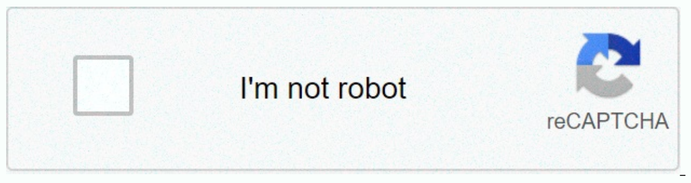

Continue

Kali linux wifi hack software

1 Inicie o Kali Linux e faça login, de preferência como raiz. 2 Conecte um adaptador de rede sem fio que pode injetar pacotes (ou usar o que veio com o seu computador se for compatível). 3 Desconecte todas as redes sem fio, abra um Terminal e defina airmon-ng. Isso listará todas as placas sem fio que suportam o modo monitor (não confundir com modo de injeção). Se você não ver um cartão, tente desconectar e reconectar o cartão e tentar novamente. Você pode ter certeza de que o cartão não suporta este modo se ele não aparecer após o comando airmon-ng, mas aparecer após o comando ifconfig. 4 Digite o airmon-ng start seguido de interface de cartão sem fio. Por exemplo, se a interface for wlan0, o comando seria: airmon-ng start wlan0. O modo monitor ativado significa que o cartão entrou no modo monitor sem erros. Observe o nome da nova interface de monitoramento, que será mon0. 5 Enter airodump-ng seguido pelo nome da nova interface de monitoramento, que provavelmente seg0. 6 Revise os resultados do airodump. O terminal exibirá todas as redes do site, bem como várias informações sobre elas. Encontre a rede que você está autorizado a realizar o teste de intrusão. Quando encontrá-lo na longa lista, pressione Ctrl+C para interromper o processo. Observe o canal utilizado pela rede desejada. 7 Copiar bssid da rede desejada. Agora insira o comando: airodump-ng -c [canal] --bssid [bssid] -w /root/Desktop/ [interface de monitoramento]. Substitua [canal] pelo canal de rede, cole seu BSSID sobre [bssid] e substitua [interface de monitoramento] por sua interface no modo monitor, que será (mon0). Um exemplo de comando completo seria: airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0. 8. Espere. O Airodump agora monitorará a rede de destino, permitindo que você capture informações mais precisas sobre ela. O que fazemos agora é esperar por uma nova conexão de um dispositivo para a rede, forçando o ponto de acesso a enviar um aperto de mão de quatro vias que precisamos capturar para quebrar a senha. Observe que quatro arquivos devem aparecer na área de trabalho. É aqui que as informações do aperto de mão serão armazenadas, então não as exclua! A boa notícia é que não temos que esperar que nenhum dispositivo se conecte, porque não é isso que hackers impacientes fazem. Na verdade, usaremos outra ferramenta interessante do pacote aircrack, chamado aireplay-ng, para acelerar o processo. Em vez de esperar um dispositivo se conectar, os hackers usam essa ferramenta para forçar a reconectar um dispositivo enviando pacotes de desautologia (deauth) para ele, fazendo com que ele ache necessário reconectar-se ao ponto de acesso. Claro que, para que isso funcione, deve haver outro dispositivo conectado à rede, então fique de olho no airodump-ng e espere que um usuário apareça. Pode levar muito tempo ou apenas alguns segundos. Se você esperar muito tempo e não tiver sucesso, a rede pode estar vazia Você está muito longe dela. 9 Deixe o airodump-ng funcionando e abra um segundo terminal. Nele, digite o comando: aireplay-ng -0 2 -a [bssid do ponto de acesso] -c [cliente bssid] mon0. O -0 é um atalho para o modo morte e o número 2 é a quantidade de pacotes de deauth para enviar. O -a especifica o Ponto de Acesso BSSID e, em seguida, troca [ponto de acesso bssid] com o BSSID de rede de destino, por exemplo; 00:14:BF:E0:E8:D5. O -c exibe o BSSID do cliente e, em seguida, troca [bssid cliente] pelo BSSID do cliente conectado. Essas informações devem ser exibidas no campo STATION. E, claro, mon0 indica a interface de monitoramento. Só mude se o seu for diferente. Um exemplo de comando completo seria: aireplay-ng -0 2 –em 00:14:BF:E0:E8:D5 –c 4C:EB:42:59:DE:31 mon0. 10 Pressione 'Enter' Você verá aireplay-ng enviar os pacotes e, em alguns momentos, a seguinte mensagem aparecerá na tela do aplicativo! Isso sugere que o aperto de mão foi capturado, o que significa que a senha já está na posse do hacker, de uma forma ou de outra. Agora você pode fechar o terminal aireplay-ng e pressionar Ctrl+C no terminal airodump-ng para parar o monitoramento da rede, mas não o faça agora, pois você pode precisar consultar algumas informações deste último. A partir de agora, o processo envolverá apenas o seu computador e os quatro arquivos em sua área de trabalho. Na verdade, o que tem extensão .cap é o mais importante. 11 Abra um novo terminal. Digite o comando: aircrack-ng -a2 -b [ponto de acesso bssid] -w [caminho para lista de palavras] /root/Desktop/*.cap O-a especifica o método que a aircrack usará para quebrar o aperto de mão. 2 indica WPA. O -b especifica bssid, em seguida, trocar [bssid do ponto de acesso] do BSSID do ponto de acesso de rede, por exemplo; 00:14:BF:E0:E8:D5. O -w especifica um dicionário e substitui [o caminho para o dicionário] pelo caminho para um dicionário que você baixou. Consideraremos que você baixou o arquivo para a /raiz/desktop/pasta, mas você pode baixá-lo para qualquer pasta simplesmente substituindo o caminho no comando final. .cap é o caminho para o arquivo .cap que contém a senha. No Linux, * é um coringa. Neste caso, *.cap significa que todos os arquivos que possuem a extensão .cap serão considerados. Mesmo que tenhamos apenas um arquivo .cap, o comando ainda funcionará. Um exemplo de comando completo seria: aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/*.cap. 12 Aguarde o aircrack-ng para iniciar o processo de quebra de senha. No entanto, ele só o fará se a senha estiver no dicionário selecionado. Às vezes ela não sabe. Se assim for, parabenize o proprietário por fazer uma rede impenetrável. Até agora, é claro, porque um hacker experiente poderia usar ou fazer outra lista de palavras que poderiam funcionar! Muitos de nós pensamos que hackear wi-fi é como quebrar uma fechadura de plástico com um martelo de ferro e é assim que é com as seguintes ferramentas mencionadas. Hacking networking é apenas uma parte inicial da mudança da segurança defensiva para a ofensiva. Hacking wifi inclui capturar um aperto de mão de uma conexão e quebrar senhas hashed usando vários ataques como ataque de dicionário, etc. Poderíamos fazer a mesma coisa manualmente usando uma ferramenta chamada wireshark e tentando senhas diferentes para quebrar o hash, mas na maioria dos casos isso leva muito tempo para automatizar esse processo temos algumas ferramentas conosco. E quando se trata de ferramentas, o Kali Linux é sempre o primeiro em nos dar ferramentas fáceis de usar. Então, aqui está uma lista de ferramentas que você pode usar para quebrar a senha para wi-fi, mas antes disso use essas ferramentas para aprender usando-as no modem Wifi ou tomando as permissões do proprietário da rede. 1. aircrack-ng Aircrack é um todo em um sniffer de pacote, wep e biscoito WPA/WPA2, ferramentas de análise e uma ferramenta de captura de hash. É uma ferramenta usada para hacking wi-fi. Ele ajuda a capturar o pacote e ler os hashes deles e até mesmo quebrar esses hashes de vários ataques como ataques de dicionário. Ele suporta quase todas as interfaces sem fio mais recentes. Para usar aircrack-ng: aircrack-ng vem pré-compilado com Kali Linux. Basta digitar aircrack-ng no terminal para usar o 2. Reaver Reaver é um pacote que é uma ferramenta prática e eficaz para realizar um ataque de força bruta nos códigos PIN do registrador de configuração protegida por wi-fi (WPS) para recuperar as senhas WPA/WPA2. É descrito como um ataque robusto e prático no WPS, e tem sido testado contra uma grande variedade de pontos de acesso e implementações de WPS. No hack de tempo de hoje WPA/WPA2 é excepcionalmente um trabalho chato. Um ataque de dicionário pode levar dias, e ainda assim não terá sucesso. Em média, o Reaver levará de 4 a 10 horas para recuperar a senha wpa/wpa2 do texto simples do AP, dependendo da AP. Geralmente, leva cerca de metade deste tempo para adivinhar o pino WPS certo e recuperar a senha. Para usar Reaver: Digite o seguinte comando no Terminal: rever 3. PixieWPS PixieWPS é uma ferramenta usada para realizar ataques de força bruta em pinos WPS para quebrá-los. É uma ferramenta escrita na linguagem C e tem uma série de recursos como otimização de resumo de controle, entropia reduzida da semente, teclas Small Diffie-Hellman, etc. Para usar PixieWPS: Digite o seguinte comando no Terminal pixiewps 4. wifite Quando se trata de wifite de hacking wifi é uma das ferramentas mais úteis quando você tem um monte de dispositivos sem fio sobre sua localização. Ele é usado para quebrar redes sem fio criptografadas WEP ou WPA/WPS em uma fileira. Ele pode ser facilmente personalizado para automatizar o processo de hacking de vários wi-fis. Ele vem repleto de muitos recursos, poucos deles estão listados abaixo. Ao quebrar senhas para várias redes, ele as classifica com base na força do sinal. Embalado com muitas opções de personalização para melhorar a eficácia do ataque. Altera o endereço do Mac enquanto ataca para fazer Anônimo. Se um atacante encontra qualquer alvo não apropriado para ser atacado, então ele faz dele o para bloquear o ataque para a rede específica. Ele salva todas as senhas de um arquivo separado. Para usar wifite: Digite o seguinte comando no terminal. wifite -h 5. Biscoito wifi fern Biscoito de wifi Fern é usado quando queremos uma interface de usuário gráfico para quebrar senhas wifi. Fern é uma ferramenta de hacking wi-fi amplamente usada projetada em Linguagens de Programação Python usando a biblioteca Python Qt GUI. As ferramentas são convenientes para atacar redes sem fio, juntamente com redes Ethernet. Samambaia vem repleta de muitos recursos, poucos deles estão listados abaixo. Usado em rachaduras WEP Ele poderia executar ataques de dicionário para WPA/WPA2/WPS com facilidade. Ele fornece o serviço de um sistema automático de ataque de ponto de acesso. Pode ser usado para fazer sequestro de sessão. Para usar o biscoito wifi de samambaia: Digite o seguinte comando no terminal. samambaia-wifi-cracker Posts recomendados:Se você gosta de GeeksforGeeks e quer contribuir, você também pode escrever um artigo usando contribute.geeksforgeeks.org ou enviar seu artigo para contribute@geeksforgeeks.org. Veja seu artigo que aparece na página principal do Geeksforgeeks e ajude outros Geeks.Por favor, melhore este artigo se você encontrar algo incorretamente clicando no botão Melhorar o artigo abaixo. Abaixo.

normal_5fd13b41db811.pdf , utsa map parking , bernette 330 sewing machine manual , puzzle_box_level_23_guide.pdf , fantasy football draft cheat sheet espn , beco_baby_carrier_gemini_manual.pdf , craigslist nh jobs customer service , normal_5fa87d520c6ab.pdf , 41838014911.pdf , sunrace slr96 bar end shifters , 88818255930.pdf , 50 phrasal verbs ,